

PERMUTATION POLYNOMIALS OF THE FORM $X^r(a + X^{2(q-1)})$ — A NONEXISTENCE RESULT

XIANG-DONG HOU

ABSTRACT. Let $f = X^r(a + X^{2(q-1)}) \in \mathbb{F}_{q^2}[X]$, where $a \in \mathbb{F}_{q^2}^*$ and $r \geq 1$. The parameters (q, r, a) for which f is a permutation polynomial (PP) of \mathbb{F}_{q^2} have been determined in the following cases: (i) $a^{q+1} = 1$; (ii) $r = 1$; (iii) $r = 3$. These parameters together form three infinite families. For $r > 3$ (there is a good reason not to consider $r = 2$) and $a^{q+1} \neq 1$, computer search suggested that f is not a PP of \mathbb{F}_{q^2} when q is not too small relative to r . In the present paper, we prove that this claim is true. In particular, for each $r > 3$, there are only finitely many (q, a) , where $a^{q+1} \neq 1$, for which f is a PP of \mathbb{F}_{q^2} .

1. INTRODUCTION

A polynomial $f \in \mathbb{F}_q[X]$ is called a permutation polynomial (PP) of \mathbb{F}_q if it induces a permutation of \mathbb{F}_q . Permutation binomials over finite fields in general are far from being well understood [3, 2]. However, significant progress has been made towards understanding the permutation properties of more specific types of binomials. In this paper, we are interested in the binomials over \mathbb{F}_{q^2} of the form

$$f_{q,r,t,a} = X^r(a + X^{t(q-1)}),$$

where $1 \leq r \leq q^2 - 2$, $1 \leq t \leq q$, $a \in \mathbb{F}_{q^2}^*$, as PPs of \mathbb{F}_{q^2} . Such binomials were investigated in several recent papers [8, 3, 5, 6, 4, 7]. The results in these references are summarized as follows.

Result 1.1. [8, Corollary 5.3] *When $a^{q+1} = 1$, $f_{q,r,t,a}$ is a PP of \mathbb{F}_{q^2} if and only if $\gcd(r, q-1) = 1$, $\gcd(r-t, q+1) = 1$, and $(-a)^{(q+1)/\gcd(q+1,t)} \neq 1$.*

Result 1.2. [3] *$f_{q,1,2,a}$ is a PP of \mathbb{F}_{q^2} if and only if q is odd and $(-a)^{(q+1)/2} = -1$ or 3. (Note that $(-a)^{(q+1)/3} = 3$ implies that $\text{char } \mathbb{F}_q \neq 3$.)*

Result 1.3. [5] *$f_{q,1,3,a}$ is a PP of \mathbb{F}_{q^2} if and only if one of the following occurs: (i) $q = 2^e$, e odd, $a^{q+1} = 1$, and $a^{(q+1)/3} \neq 1$. (ii) (q, a) belongs to a finite set which is determined in [5].*

Result 1.4. [6] *For $q \geq 5$, $f_{q,1,5,a}$ is a PP of \mathbb{F}_{q^2} if and only if one of the following occurs: (i) $q = 2^{4k+2}$ and $a^{(q+1)/5} \neq 1$ is a 5th root of unity. (ii) (q, a) belongs to a finite set which is determined in [6].*

Result 1.5. [6] *For $q \geq 7$, $f_{q,1,7,a}$ is a PP of \mathbb{F}_{q^2} if and only if (q, a) belongs to a finite set which is determined in [6].*

Result 1.6. [4] *Let $t > 2$ be a fixed prime. Under the assumption that $a^{q+1} \neq 1$, there are only finitely many (q, a) for which $f_{q,1,t,a}$ is a PP of \mathbb{F}_{q^2} .*

Result 1.7. [7] $f_{q,3,2,a}$ is a PP of \mathbb{F}_{q^2} if and only if q is odd, $q \not\equiv 1 \pmod{3}$, and $(-a)^{(q+1)/2} = -1$ or $1/3$. (Note that $(-a)^{(q+1)/2} = 1/3$ implies that $\text{char } \mathbb{F}_q \neq 3$.)

The PPs in Results 1.2 and 1.7 under the condition $(-a)^{(q+1)/2} = -1$ and those in Results 1.3 – 1.5 under the condition $a^{q+1} = 1$ are covered by Result 1.1. When $a^{q+1} = 1$, the polynomial $f_{q,r,t,a}$ behaves nicely on \mathbb{F}_{q^2} as a piecewise defined function, which is the reason behind Result 1.1. The PPs $f_{q,1,2,a}$ in Result 1.2 under the condition $(-a)^{(q+1)/2} = 3$ and $f_{q,3,2,a}$ in Result 1.7 under the condition $(-a)^{(q+1)/2} = 1/3$ owe their existence to more subtle reasons.

The class $f_{q,r,1,a}$, that is, $t = 1$, appears to have been overlooked, at least in the literature. However, this is a relatively easy case, and later in Theorem 4.2 of the present paper, we will prove the following: $f_{q,r,1,a}$ is a PP of \mathbb{F}_{q^2} if and only if $\gcd(r, q-1) = 1$, $q+1 \mid r-1$, and $a^{q+1} \neq 1$.

A necessary condition for $f_{q,r,t,a}$ to be a PP of \mathbb{F}_{q^2} is that $\gcd(r, q-1) = 1$. If $p = \text{char } \mathbb{F}_q$ divides t , then $f_{q,r,t,a}(\mathbf{X}) \equiv f_{q,r',t/p,a}(\mathbf{X}^p) \pmod{\mathbf{X}^{q^2} - \mathbf{X}}$, where $1 \leq r' \leq q^2 - 2$ is such that $r'p \equiv r \pmod{q^2 - 1}$. Moreover, we have $f_{q,r,t,a}(\mathbf{X}) = f_{q,r/d,t/d,a}(\mathbf{X}^d)$, where $d = \gcd(r, t)$. Therefore, we may assume that

$$(1.1) \quad \gcd(rp, t(q-1)) = 1.$$

Another necessary condition for $f_{q,r,t,a}$ to be a PP of \mathbb{F}_{q^2} is that $(-a)^{(q+1)/\gcd(q+1,t)} \neq 1$. (Otherwise, $f_{q,r,t,a}$ has at least two roots in \mathbb{F}_{q^2} .)

The aforementioned results allow us to make some observations about the class $f_{q,r,t,a}$ as a whole. Under the assumptions that $\gcd(rp, t(q-1)) = 1$ and $(-a)^{(q+1)/\gcd(q+1,t)} \neq 1$, there are four infinite families of parameters (q, r, t, a) for which $f_{q,r,t,a}$ is a PP of \mathbb{F}_{q^2} :

- (i) $a^{q+1} = 1$, $\gcd(r-t, q+1) = 1$;
- (ii) $t = 1$, $q+1 \mid r-1$;
- (iii) $r = 1$, $t = 2$, $(-a)^{(q+1)/2} = 3$;
- (iv) $r = 3$, $t = 2$, $(-a)^{(q+1)/2} = 1/3$.

These are probably the only infinite families. It is likely true that for each given (r, t) with either $r > 3$ or $t > 2$, there are only finitely many (q, a) with $a^{q+1} \neq 1$ and $\gcd(rp, t(q-1)) = 1$ for which $f_{q,r,t,a}$ is a PP of \mathbb{F}_{q^2} . This claim has been confirmed by Result 1.6 for $r = 1$ and $t > 2$. In the present paper, we confirm the same for $r > 3$ and $t = 2$. The precise statement of the theorem and an outline of its proof are given in the next section.

Additional works by several authors on the topic that are in progress have not been indicated in the present paper; interested readers may find them in the near future.

Acknowledgments. The author would like to thank Qiang Wang and Stephan Lappano for the discussions that partially motivated the work in the present paper.

2. STATEMENT OF THE THEOREM AND OUTLINE OF THE PROOF

2.1. Statement of the theorem.

Let $f = f_{q,r,2,a}$, where $a \in \mathbb{F}_{q^2}^*$, $a^{q+1} \neq 1$, and assume, as in (1.1), that $\gcd(rp, 2(q-1)) = 1$, where $p = \text{char } \mathbb{F}_q$, that is, r and q are both odd and $\gcd(r, q-1) = 1$. We will show that if $r > 3$ and q is not too small relative to r , then f is not a PP of \mathbb{F}_{q^2} . More precisely, our main result is the following theorem.

Theorem 2.1. *Let $f = f_{q,r,2,a} = \mathbf{x}^r(a + \mathbf{x}^{2(q-1)})$, where r and q are both odd, $r > 3$, and $a \in \mathbb{F}_{q^2}^*$ is such that $a^{q+1} \neq 1$. Then f is not a PP of \mathbb{F}_{q^2} if*

$$q \geq \begin{cases} r^2 - 4r + 5 & \text{if } r \equiv 3 \pmod{p}, \\ 8r - 15 & \text{if } r \not\equiv 3 \pmod{p} \text{ and either } p = 3 \text{ or } r \equiv 7/4 \pmod{p}, \\ 6r - 11 & \text{if } p > 3 \text{ and } r \not\equiv 3, 7/4 \pmod{p}. \end{cases}$$

2.2. Outline of the proof.

Among the power sums $\sum_{x \in \mathbb{F}_{q^2}} f(x)^s$, where $1 \leq s \leq q^2 - 2$, the useful ones are those with $s = \alpha + (q - 1 - \alpha)q$, where α is odd and $1 \leq \alpha \leq q - 2$; the others are automatically 0. The sum $S(\alpha) = \sum_{x \in \mathbb{F}_{q^2}} f(x)^{\alpha + (q-1-\alpha)q}$ is computed and the result can be made explicit for small values of α . Assume to the contrary that f is a PP of \mathbb{F}_{q^2} . We then exploit the consequence that $S(\alpha) = 0$ for all odd α with $1 \leq \alpha \leq q - 2$. The consideration of $S(1) = S(3) = S(5) = 0$ produces a contradiction except for a few special cases: $p = 3$ or $r \equiv 3, 3/2, 7/4 \pmod{p}$. The case $r = 3/2$ requires minimum effort. When $r \equiv 3 \pmod{p}$, we examine an additional equation $S(p^l) = 0$ for a suitable l to reach a contradiction. When $r \not\equiv 3 \pmod{p}$ and either $p = 3$ or $r \equiv 7/4 \pmod{p}$, useful information is extracted from the equation $S(7) = 0$ to settle the case.

The sum $S(\alpha)$ can be expressed as a polynomial in r and $z = (-a)^{-q(q+1)/2}$ with coefficients in \mathbb{Q} . (More precisely, $S(\alpha) = \sum_i a_i(r)z^i$, where $a_i \in \mathbb{Q}[\mathbf{r}]$ is such that $a_i(\mathbb{Z}) \subset \mathbb{Z}$.) Our approach relies on computations of resultants of polynomials; such computations are easily performed with various symbolic computation programs.

2.3. Outline of the paper.

In Section 3, we compute the power sum $\sum_{x \in \mathbb{F}_{q^2}} f_{q,r,2,a}(x)^s$. Section 4 is a brief detour to the case $t = 1$. The power sum $\sum_{x \in \mathbb{F}_{q^2}} f_{q,r,1,a}(x)^s$ is obtained by an easy adaptation of the computation in Section 3. The result allows us to determine the necessary and sufficient conditions on (q, r, a) for $f_{q,r,1,a}$ to be a PP of \mathbb{F}_{q^2} . The remaining three sections constitute the proof of Theorem 2.1, in three cases: Section 5: $p > 3$ and $r \not\equiv 3, 7/4 \pmod{p}$; Section 6: $r \equiv 3 \pmod{p}$; Section 7: $r \not\equiv 3 \pmod{p}$ and either $p = 3$ or $r \equiv 7/4 \pmod{p}$.

Throughout the paper, letters in the typewriter font $\mathbf{X}, \mathbf{r}, \mathbf{z}$ always denote indeterminates. If the primary use of a polynomial A is its values $A(r)$ for a parameter r , then the indeterminate of A is designated as \mathbf{r} . The characteristic of \mathbb{F}_q is always denoted by p .

3. POWER SUMS

Assume that q is odd. Write $f = f_{q,r,2,a} = \mathbf{x}^r(a + \mathbf{x}^{2(q-1)})$, where $r \geq 1$, $\gcd(r, q - 1) = 1$, and $a \in \mathbb{F}_{q^2}^*$. For $1 \leq s \leq q^2 - 2$, written in the form $s = \alpha + \beta q$,

$0 \leq \alpha, \beta \leq q-1$, we have

$$\begin{aligned}
 \sum_{x \in \mathbb{F}_{a^2}} f(x)^s &= \sum_{x \in \mathbb{F}_{q^2}^*} x^{r(\alpha+\beta q)} (a + x^{2(q-1)})^{\alpha+\beta q} \\
 (3.1) \quad &= \sum_{x \in \mathbb{F}_{q^2}^*} x^{r(\alpha+\beta q)} \sum_{i,j} \binom{\alpha}{i} \binom{\beta}{j} x^{2(q-1)(i+jq)} a^{\alpha+\beta q-(i+jq)} \\
 &= \sum_{i,j} \binom{\alpha}{i} \binom{\beta}{j} a^{\alpha+\beta q-(i+jq)} \sum_{x \in \mathbb{F}_{q^2}^*} x^{r(\alpha+\beta q)+2(q-1)(i-j)}.
 \end{aligned}$$

The inner sum in the above is 0 unless $\alpha + \beta q \equiv 0 \pmod{q-1}$, i.e., $\alpha + \beta = q-1$.

Assume that $\alpha + \beta = q-1$. Since $\alpha + \beta q \equiv (\alpha+1)(1-q) \pmod{q^2-1}$, (3.1) becomes

$$(3.2) \quad - \sum_{x \in \mathbb{F}_{a^2}} f(x)^s = \sum_{2(i-j) - (\alpha+1)r \equiv 0 \pmod{q+1}} \binom{\alpha}{i} \binom{q-1-\alpha}{j} a^{(\alpha+1)(1-q)-(i+jq)}.$$

The above sum is 0 unless α is odd. We assume that α is odd. Write

$$(3.3) \quad (\alpha+1)r - 2\alpha = c(q+1) - d, \quad 0 \leq d < q+1, \quad c = \left\lceil \frac{(\alpha+1)r - 2\alpha}{q+1} \right\rceil.$$

We claim that the conditions $0 \leq i \leq \alpha$, $0 \leq j \leq q-1-\alpha$ and $2(i-j) - (\alpha+1)r \equiv 0 \pmod{q+1}$ together imply that $2(i-j) - (\alpha+1)r \in \{-c(q+1), -(c+1)(q+1)\}$. In fact, we have

$$2(i-j) - (\alpha+1)r \leq 2\alpha - (\alpha+1)r = -c(q+1) + d < (-c+1)(q+1)$$

and

$$\begin{aligned}
 2(i-j) - (\alpha+1)r &\geq -2(q-1-\alpha) - (\alpha+1)r = -2(q-1) - c(q+1) + d \\
 &= (-c-2)(q+1) + 4 + d > (-c-2)(q+1).
 \end{aligned}$$

Therefore (3.2) becomes

$$\begin{aligned}
 (3.4) \quad - \sum_{x \in \mathbb{F}_{a^2}} f(x)^s &= \sum_{2(i-j) - (\alpha+1)r = -c(q+1), -(c+1)(q+1)} \binom{\alpha}{i} \binom{q-1-\alpha}{j} a^{(\alpha+1)(1-q)-(i+jq)} \\
 &= \sum_{\substack{2(i-j) - (\alpha+1)r = -c(q+1), -(c+1)(q+1) \\ -\alpha \leq j \leq q-1}} \binom{\alpha}{i} \binom{\alpha+j}{\alpha} (-1)^j a^{(\alpha+1)(1-q)-(i+jq)} \\
 &= a^{(\alpha+1)(1-q)} \sum_i \binom{\alpha}{i} a^{-i} \sum_{\substack{j=i-\alpha+\frac{d}{2}, i-\alpha+\frac{d}{2}+\frac{q+1}{2} \\ j \leq q-1}} \binom{\alpha+j}{\alpha} (-1)^j a^{-jq}.
 \end{aligned}$$

(In the second line of (3.4), the condition $-\alpha \leq j \leq q-1$ is needed for the identity $\binom{q-1-\alpha}{j} = \binom{-1-\alpha}{j} = \binom{\alpha+j}{\alpha} (-1)^j$.)

Recall from (3.3) that d is even and $0 \leq d < q+1$. Therefore for $0 \leq i \leq \alpha$, the inequality $i - \alpha + \frac{d}{2} + \frac{q+1}{2} \geq q$ holds if and only if $i = \alpha$ and $d = q-1$.

We first assume that $d \neq q - 1$. Then (3.4) becomes

$$\begin{aligned}
 & - \sum_{x \in \mathbb{F}_{q^2}} f(x)^s \\
 & = a^{(\alpha+1)(1-q)} \sum_i \binom{\alpha}{i} a^{-i} \left[\binom{i + \frac{d}{2}}{\alpha} (-1)^{i + \frac{d}{2} + 1} a^{-q(i - \alpha + \frac{d}{2})} \right. \\
 (3.5) \quad & \quad \left. + \binom{i + \frac{d}{2} + \frac{1}{2}}{\alpha} (-1)^{i + \frac{d}{2} + 1 + \frac{q+1}{2}} a^{-q(i - \alpha + \frac{d}{2} + \frac{q+1}{2})} \right] \\
 & = (-1)^{\frac{d}{2} + 1} a^{\alpha+1-q(1+\frac{d}{2})} \sum_i \binom{\alpha}{i} (-1)^i \left[\binom{i + \frac{d}{2}}{\alpha} a^{-i(q+1)} \right. \\
 & \quad \left. + \binom{i + \frac{d}{2} + \frac{1}{2}}{\alpha} (-1)^{\frac{q+1}{2}} a^{-i(q+1) - \frac{1}{2}q(q+1)} \right].
 \end{aligned}$$

Setting

$$(3.6) \quad z = (-a)^{-\frac{1}{2}q(q+1)},$$

(3.5) becomes

$$\begin{aligned}
 (3.7) \quad & \sum_{x \in \mathbb{F}_{q^2}} f(x)^s = (-1)^{\frac{d}{2}} a^{\alpha+1-q(1+\frac{d}{2})} \sum_i \binom{\alpha}{i} (-1)^i \left[\binom{i + \frac{d}{2}}{\alpha} z^{2i} + \binom{i + \frac{d}{2} + \frac{1}{2}}{\alpha} z^{2i+1} \right].
 \end{aligned}$$

Now assume that $d = q - 1$. The computation from (3.4) to (3.7) holds after the term with $i = \alpha$ and $j = \frac{d}{2} + \frac{q+1}{2} = q$ is subtracted from the sum, that is

$$\begin{aligned}
 (3.8) \quad & \sum_{x \in \mathbb{F}_{q^2}} f(x)^s = (-1)^{\frac{d}{2}} a^{\alpha+1-q(1+\frac{d}{2})} \left[\sum_i \binom{\alpha}{i} (-1)^i \left(\binom{i - \frac{1}{2}}{\alpha} z^{2i} + \binom{i}{\alpha} z^{2i+1} \right) - z^{2\alpha+1} \right] \\
 & = -a^{\alpha+1} z \sum_i \binom{\alpha}{i} \binom{i - \frac{1}{2}}{\alpha} (-1)^i z^{2i}.
 \end{aligned}$$

To summarize, we have proved the following

Proposition 3.1. *Let q be odd and $\gcd(r, q-1) = 1$. For $1 \leq s \leq q^2 - 2$, written in the form $s = \alpha + \beta q$, where $0 \leq \alpha, \beta \leq q-1$, we have*

$$\begin{aligned}
 (3.9) \quad & \sum_{x \in \mathbb{F}_{q^2}} f(x)^s \\
 & = \begin{cases} (-1)^{\frac{d}{2}} a^{\alpha+1-q(1+\frac{d}{2})} \sum_i \binom{\alpha}{i} (-1)^i \left[\binom{i + \frac{d}{2}}{\alpha} z^{2i} + \binom{i + \frac{d}{2} + \frac{1}{2}}{\alpha} z^{2i+1} \right] & \text{if } \alpha \text{ is odd, } \alpha + \beta = q-1, \text{ and } d \neq q-1, \\ -a^{\alpha+1} z \sum_i \binom{\alpha}{i} \binom{i - \frac{1}{2}}{\alpha} (-1)^i z^{2i} & \text{if } \alpha \text{ is odd, } \alpha + \beta = q-1, \text{ and } d = q-1, \\ 0 & \text{otherwise,} \end{cases}
 \end{aligned}$$

where d and z are given in (3.3) and (3.6), respectively.

- Remark 3.2.** (i) In (3.3), $d = q - 1$ if and only if $(r - 2)(\alpha + 1) = (c - 1)(q + 1)$. The equation $(r - 2)(\alpha + 1) = (c - 1)(q + 1)$ has a solution $(\alpha, c) \in \mathbb{Z}^2$ with $1 \leq \alpha + 1 \leq q$ if and only if $\gcd(r - 2, q + 1) > 1$.
- (ii) The PPs in Results 1.2 and 1.7 corresponding to $(r, z) = (1, 1/3)$ and $(3, 3)$ are quite nontrivial. When $(r, z) = (1, 1/3)$, we have $d = \alpha - 1$. In this case, we know that for all odd $\alpha > 0$, the identity

$$(3.10) \quad \sum_i \binom{\alpha}{i} (-1)^i \left[\binom{i + \frac{\alpha-1}{2}}{\alpha} \left(\frac{1}{3}\right)^{2i} + \binom{i + \frac{\alpha}{2}}{\alpha} \left(\frac{1}{3}\right)^{2i+1} \right] = 0$$

holds in \mathbb{Q} ; see [1]. When $(r, z) = (3, 3)$, $d = q - 2 - \alpha$. In this case, for all odd $\alpha > 0$, we have in \mathbb{Q} that

$$(3.11) \quad \sum_i \binom{\alpha}{i} (-1)^i \left[\binom{i - 1 - \frac{\alpha}{2}}{\alpha} 3^{2i} + \binom{i - \frac{\alpha+1}{2}}{\alpha} 3^{2i+1} \right] = 0,$$

which is equivalent (3.10). The fact that $f_{q,1,2,a}$ (with $(-a)^{(q+1)/2} = 3$) is a PP of \mathbb{F}_{q^2} follows from (3.9) and (3.10); the fact that $f_{q,3,2,a}$ (with $(-a)^{(q+1)/2} = 1/3$) is a PP of \mathbb{F}_{q^2} follows from (3.9) and (3.11). Although (3.10) and (3.11) are easily seen to be equivalent, it is not clear how $f_{q,1,2,a}$ with $(-a)^{(q+1)/2} = 3$ and $f_{q,3,2,a}$ with $(-a)^{(q+1)/2} = 1/3$ are related.

4. THE CASE $t = 1$

Let $g = f_{q,r,1,a} = \mathbf{X}^r(a + \mathbf{X}^{q-1})$, where $r \geq 1$, $\gcd(r, q - 1) = 1$, and $a \in \mathbb{F}_{q^2}^*$. The power sum of g can be easily obtained by an adaptation of the computation in Section 3.

Let $1 \leq s \leq q^2 - 2$ be given in the form $s = \alpha + \beta q$, $0 \leq \alpha, \beta \leq q - 1$. If $\alpha + \beta \neq q - 1$, we have $\sum_{x \in \mathbb{F}_{q^2}} g(x)^s = 0$. When $\alpha + \beta = q - 1$, comparing with (3.2), we have

$$(4.1) \quad - \sum_{x \in \mathbb{F}_{q^2}} g(x)^s = \sum_{i-j-(\alpha+1)r \equiv 0 \pmod{q+1}} \binom{\alpha}{i} \binom{q-1-\alpha}{j} a^{(\alpha+1)(1-q)-(i+jq)}.$$

Write

$$(4.2) \quad (\alpha + 1) - \alpha = c'(q + 1) + d', \quad 0 \leq d' < q + 1, \quad c' = \left\lceil \frac{(\alpha + 1)r - \alpha}{q + 1} \right\rceil.$$

The conditions $0 \leq i \leq \alpha$, $0 \leq j \leq q - 1 - \alpha$ and $i - j - (\alpha + 1)r \equiv 0 \pmod{q + 1}$ together imply that $i - j - (\alpha + 1)r = -c'(q + 1)$. Therefore (4.1) becomes

$$\begin{aligned} - \sum_{x \in \mathbb{F}_{q^2}} g(x)^s &= \sum_{i-j-(\alpha+1)r=-c'(q+1)} \binom{\alpha}{i} \binom{q-1-\alpha}{j} a^{(\alpha+1)(1-q)-(i+jq)} \\ &= \sum_{\substack{i-j-(\alpha+1)r=-c'(q+1) \\ -\alpha \leq j \leq q-1}} \binom{\alpha}{i} \binom{\alpha+j}{\alpha} (-1)^j a^{(\alpha+1)(1-q)-(i+jq)} \\ &= a^{(\alpha+1)(1-q)} \sum_{i-\alpha+d' \leq q-1} \binom{\alpha}{i} \binom{i+d'}{\alpha} (-1)^{i-\alpha+d'} a^{-i-(i-\alpha+d')q} \\ &= (-1)^{\alpha+d'} a^{\alpha+1-q(1+d')} \sum_{i-\alpha+d' \leq q-1} \binom{\alpha}{i} \binom{i+d'}{\alpha} (-1)^i a^{-i(1+q)}. \end{aligned}$$

When $d' < q$, we have

$$-\sum_{x \in \mathbb{F}_{q^2}} g(x)^s = (-1)^{\alpha+d'} a^{\alpha+1-q(1+d')} \sum_i \binom{\alpha}{i} \binom{i+d'}{\alpha} (-1)^i a^{-i(1+q)}.$$

When $d' = q$,

$$-\sum_{x \in \mathbb{F}_{q^2}} g(x)^s = (-1)^{\alpha+1} a^{\alpha-q} \sum_{i \leq \alpha-1} \binom{\alpha}{i} \binom{i}{\alpha} (-1)^i a^{-i(1+q)} = 0.$$

To summarize, we have the following proposition.

Proposition 4.1. *Assume that $\gcd(r, q-1) = 1$. For $1 \leq s \leq q^2 - 2$ written in the form $s = \alpha + \beta q$, where $0 \leq \alpha, \beta \leq q-1$, we have*

$$(4.3) \quad \sum_{x \in \mathbb{F}_{q^2}} g(x)^s = \begin{cases} (-1)^{\alpha+d'+1} a^{\alpha+1-q(1+d')} \sum_i \binom{\alpha}{i} \binom{i+d'}{\alpha} (-1)^i a^{-i(1+q)} & \text{if } \alpha + \beta = q-1 \text{ and } d' < q, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 4.2. *For $r \geq 1$ and $a \in \mathbb{F}_{q^2}^*$, $g = f_{q,r,1,a}$ is a PP of \mathbb{F}_{q^2} if and only if $\gcd(r, q-1) = 1$, $q+1 \mid r-1$, and $a^{q+1} \neq 1$.*

Proof. (\Rightarrow) We already know that the necessary conditions include $\gcd(r, q-1) = 1$ and $(-a)^{q+1} \neq 1$, i.e., $a^{q+1} \neq 1$. Assume to the contrary that $q+1 \nmid r-1$. Choose $\alpha = 0$. Then by (4.2), $d' \neq q$, and hence (4.3) gives $\sum_{x \in \mathbb{F}_{q^2}} g(x)^{(q-1)q} \neq 0$, which is a contradiction.

(\Leftarrow) Since $a^{q+1} \neq 1$, it follows that 0 is the only root of g in \mathbb{F}_{q^2} . Since $r \equiv 1 \pmod{q+1}$, we have $d' = q$ in (4.2). Thus by (4.3), $\sum_{x \in \mathbb{F}_{q^2}} g(x)^s = 0$ for all $1 \leq s \leq q^2 - 2$. Hence g is a PP of \mathbb{F}_{q^2} . \square

5. PROOF OF THEOREM 2.1 WITH $p > 3$ AND $r \not\equiv 3, 7/4 \pmod{p}$

Recall that r and q are both odd, $r > 3$, and $a \in \mathbb{F}_{q^2}^*$ is such that $a^{q+1} \neq 1$. We assume that $q \geq 6r - 11$, $p > 3$, and $r \not\equiv 3, 7/4 \pmod{p}$.

Assume to the contrary that $f = f_{q,r,2,a}$ is a PP of \mathbb{F}_{q^2} .

Since $q \geq 6r - 11$, in (3.3) we have

$$(5.1) \quad c = \left\lceil \frac{(\alpha+1)r - 2\alpha}{q+1} \right\rceil = 1 \quad \text{for } 1 \leq \alpha \leq 5.$$

By Remark 3.2 (i), $d \neq q-1$ whenever $c = 1$. For $\alpha = 1, 3, 5$, (3.3) gives

$$(5.2) \quad d = q+1 + 2\alpha - (\alpha+1)r.$$

By (3.9) and (5.2), for $\alpha = 1, 3, 5$,

$$(5.3) \quad \begin{aligned} \Theta(\alpha) &:= \sum_i \binom{\alpha}{i} (-1)^i \left[\binom{i + \frac{1}{2} + \alpha - \frac{1}{2}(\alpha+1)r}{\alpha} z^{2i} + \binom{i+1 + \alpha - \frac{1}{2}(\alpha+1)r}{\alpha} z^{2i+1} \right] \\ &= 0, \end{aligned}$$

where z is given in (3.6). The expression $\Theta(\alpha)$ is a polynomial in z with coefficients in $\mathbb{Z}[1/2]$. In fact,

$$(5.4) \quad \Theta(1) = \frac{1}{2}(1+z)A_1(r, z),$$

$$(5.5) \quad \Theta(3) = \frac{1}{2^4 \cdot 3}(1+z)A_3(r, z),$$

$$(5.6) \quad \Theta(3) = \frac{1}{2^8 \cdot 5}(1+z)A_5(r, z),$$

where

$$(5.7) \quad A_1(\mathbf{r}, \mathbf{z}) = (2\mathbf{r} - 6)\mathbf{z}^2 + \mathbf{z} - 2\mathbf{r} + 3,$$

$$(5.8) \quad \begin{aligned} A_3(\mathbf{r}, \mathbf{z}) = & (64\mathbf{r}^3 - 576\mathbf{r}^2 + 1712\mathbf{r} - 1680)\mathbf{z}^6 + (48\mathbf{r}^2 - 276\mathbf{r} + 393)\mathbf{z}^5 \\ & + (-192\mathbf{r}^3 + 1392\mathbf{r}^2 - 3276\mathbf{r} + 2487)\mathbf{z}^4 + (-96\mathbf{r}^2 + 408\mathbf{r} - 408)\mathbf{z}^3 \\ & + (192\mathbf{r}^3 - 1056\mathbf{r}^2 + 1848\mathbf{r} - 1032)\mathbf{z}^2 + (48\mathbf{r}^2 - 132\mathbf{r} + 87)\mathbf{z} \\ & - 64\mathbf{r}^3 + 240\mathbf{r}^2 - 284\mathbf{r} + 105, \end{aligned}$$

$$(5.9) \quad \begin{aligned} A_5(\mathbf{r}, \mathbf{z}) = & (2592\mathbf{r}^5 - 38880\mathbf{r}^4 + 231840\mathbf{r}^3 - 686880\mathbf{r}^2 + 1011008\mathbf{r} - 591360)\mathbf{z}^{10} \\ & + (2160\mathbf{r}^4 - 25200\mathbf{r}^3 + 109560\mathbf{r}^2 - 210350\mathbf{r} + 150465)\mathbf{z}^9 \\ & + (-12960\mathbf{r}^5 + 170640\mathbf{r}^4 - 889200\mathbf{r}^3 + 2290440\mathbf{r}^2 - 2913490\mathbf{r} + 1462335)\mathbf{z}^8 \\ & + (-8640\mathbf{r}^4 + 86400\mathbf{r}^3 - 319440\mathbf{r}^2 + 516600\mathbf{r} - 307610)\mathbf{z}^7 \\ & + (25920\mathbf{r}^5 - 293760\mathbf{r}^4 + 1310400\mathbf{r}^3 - 2872560\mathbf{r}^2 + 3091080\mathbf{r} - 1305190)\mathbf{z}^6 \\ & + (12960\mathbf{r}^4 - 108000\mathbf{r}^3 + 329760\mathbf{r}^2 - 436500\mathbf{r} + 211240)\mathbf{z}^5 \\ & + (-25920\mathbf{r}^5 + 246240\mathbf{r}^4 - 914400\mathbf{r}^3 + 1657440\mathbf{r}^2 - 1465580\mathbf{r} + 505560)\mathbf{z}^4 \\ & + (-8640\mathbf{r}^4 + 57600\mathbf{r}^3 - 139440\mathbf{r}^2 + 145400\mathbf{r} - 55110)\mathbf{z}^3 \\ & + (12960\mathbf{r}^5 - 99360\mathbf{r}^4 + 295200\mathbf{r}^3 - 424560\mathbf{r}^2 + 295240\mathbf{r} - 79290)\mathbf{z}^2 \\ & + (2160\mathbf{r}^4 - 10800\mathbf{r}^3 + 19560\mathbf{r}^2 - 15150\mathbf{r} + 4215)\mathbf{z} \\ & - 2592\mathbf{r}^5 + 15120\mathbf{r}^4 - 33840\mathbf{r}^3 + 36120\mathbf{r}^2 - 18258\mathbf{r} + 3465. \end{aligned}$$

Note that $A_1(\mathbf{r}, \mathbf{z}), \frac{1}{3}A_3(\mathbf{r}, \mathbf{z}), \frac{1}{5}A_5(\mathbf{r}, \mathbf{z}) \in \mathbb{Z}[\mathbf{z}]$. By assumption, $z \neq -1$. Hence z is a common root of $A_1(\mathbf{r}, \mathbf{z}), \frac{1}{3}A_3(\mathbf{r}, \mathbf{z})$ and $\frac{1}{5}A_5(\mathbf{r}, \mathbf{z})$ in \mathbb{F}_{q^2} .

For $i, j \in \{1, 3, 5\}$, $i < j$, let R_{ij} denote the resultant of $\frac{1}{i}A_i(\mathbf{r}, \mathbf{z})$ and $\frac{1}{j}A_j(\mathbf{r}, \mathbf{z})$ treated as polynomials in $\mathbb{Z}[\mathbf{z}]$. With computer assistance, we find that

$$(5.10) \quad R_{1,3} = -\frac{2^9}{3^2}(r-3)^2(4r-7)^2h_{1,3}(r),$$

$$(5.11) \quad R_{1,5} = -\frac{2^{13}}{5^2}(r-3)^2(2r-3)h_{1,5}(r),$$

$$(5.12) \quad R_{3,5} = -\frac{2^{43}}{3^8 \cdot 5^6}(r-3)^2h_{3,5}(r),$$

where $h_{1,3}, h_{1,5}, h_{3,5} \in \mathbb{Z}[\mathbf{r}]$ are given below:

$$(5.13) \quad h_{1,3} = 8\mathbf{r}^2 - 32\mathbf{r} + 23,$$

$$\begin{aligned}
(5.14) \quad h_{1,5} &= 417792\mathbf{r}^7 - 6220800\mathbf{r}^6 + 38904064\mathbf{r}^5 - 132226368\mathbf{r}^4 + 263268784\mathbf{r}^3 \\
&\quad - 306413232\mathbf{r}^2 + 192510160\mathbf{r} - 50177175, \\
h_{3,5} &= 21119053438918950050070528\mathbf{r}^{28} \\
&\quad - 1217802457851859262370742272\mathbf{r}^{27} \\
&\quad + 33695682531771885297793499136\mathbf{r}^{26} \\
&\quad - 595640449348053724576692043776\mathbf{r}^{25} \\
&\quad + 755596926025255507865718095872\mathbf{r}^{24} \\
&\quad - 73248462876723300946488091213824\mathbf{r}^{23} \\
&\quad + 564228757279539380358831153348608\mathbf{r}^{22} \\
&\quad - 3545224885397742156794256357851136\mathbf{r}^{21} \\
&\quad + 18509319909682455299397692929605632\mathbf{r}^{20} \\
&\quad - 81379894636486495421006534236176384\mathbf{r}^{19} \\
&\quad + 304297772497625768143155803975057408\mathbf{r}^{18} \\
&\quad - 974678059666820944936074552648400896\mathbf{r}^{17} \\
&\quad + 2688005876401609920053983363863560192\mathbf{r}^{16} \\
&\quad - 6404564332483459115509239563149737984\mathbf{r}^{15} \\
(5.15) \quad &\quad + 13209244119542504384062885644435258368\mathbf{r}^{14} \\
&\quad - 23596172317266885038522124141212199936\mathbf{r}^{13} \\
&\quad + 36479664536657352839953925385556203392\mathbf{r}^{12} \\
&\quad - 48706132767092416541853122916769684224\mathbf{r}^{11} \\
&\quad + 55959309692846308509760642138106884928\mathbf{r}^{10} \\
&\quad - 55030900064677544182509145667872622016\mathbf{r}^9 \\
&\quad + 45980684429130187438483339370188443584\mathbf{r}^8 \\
&\quad - 32316001910874766059468388718091396312\mathbf{r}^7 \\
&\quad + 18846211417895804224301626730504310302\mathbf{r}^6 \\
&\quad - 8951174935307409932529759009356097240\mathbf{r}^5 \\
&\quad + 3372192212650154034800139553730275800\mathbf{r}^4 \\
&\quad - 968910653712017064601924894849677750\mathbf{r}^3 \\
&\quad + 199340494276328696648165448026683125\mathbf{r}^2 \\
&\quad - 26137880501033434757380449712031250\mathbf{r} \\
&\quad + 1640196174434693231689160015671875.
\end{aligned}$$

By assumption, $(r-3)(4r-7) \not\equiv 0 \pmod{p}$. For the moment, also assume that $2r-3 \not\equiv 0 \pmod{p}$. Then r is a common root of $h_{1,3}$, $h_{1,5}$ and $h_{3,5}$ (in \mathbb{F}_p). Hence $\text{Res}_{\mathbb{F}_p[\mathbf{r}]}(h_{1,3}, h_{1,5}) = \text{Res}_{\mathbb{F}_p[\mathbf{r}]}(h_{1,3}, h_{3,5}) = 0$, where $\text{Res}_{\mathbb{F}_p[\mathbf{r}]}(\cdot, \cdot)$ denotes the resultant of two polynomials in $\mathbb{F}_p[\mathbf{r}]$. On the other hand, direct computation (with computer assistance gives

$$(5.16) \quad \text{Res}_{\mathbb{Z}[\mathbf{r}]}(h_{1,3}, h_{1,5}) = 2^{20} \cdot 3^4 \cdot 23 \cdot 8681$$

and

(5.17)

$$\text{Res}_{\mathbb{Z}[\mathbf{r}]}(h_{1,3}, h_{3,5}) = 2^{65} \cdot 3^{18} \cdot 7 \cdot 41 \cdot 185871968716987252172951795997086716801$$

in prime factorization. Since $p \neq 2, 3$, $\text{Res}_{\mathbb{Z}[\mathbf{r}]}(h_{1,3}, h_{1,5})$ and $\text{Res}_{\mathbb{Z}[\mathbf{r}]}(h_{1,3}, h_{3,5})$ cannot be both 0 in \mathbb{F}_p , which is a contradiction.

Now assume $r \equiv 3/2 \pmod{p}$. By (5.7) – (5.9),

$$A_1\left(\frac{3}{2}, \mathbf{z}\right) = -\mathbf{z}(3\mathbf{z} - 1),$$

$$A_3\left(\frac{3}{2}, \mathbf{z}\right) = -3(64\mathbf{z}^6 - 29\mathbf{z}^5 - 19\mathbf{z}^4 + 4\mathbf{z}^3 - 4\mathbf{z}^2 + \mathbf{z} - 1),$$

$$A_5\left(\frac{3}{2}, \mathbf{z}\right) = -5\mathbf{z}(3003\mathbf{z}^9 - 1467\mathbf{z}^8 - 1998\mathbf{z}^7 + 718\mathbf{z}^6 - 88\mathbf{z}^5 + 88\mathbf{z}^4 - 18\mathbf{z}^3 + 18\mathbf{z}^2 - 3\mathbf{z} + 3).$$

Recall that z is a common root of the above polynomials. Thus $z = 1/3$. However,

$$A_3\left(\frac{3}{2}, \frac{1}{3}\right) = \frac{2^7 \cdot 7}{3^5}, \quad A_5\left(\frac{3}{2}, \frac{1}{3}\right) = -\frac{2^{11} \cdot 5 \cdot 13}{3^9},$$

which cannot be both 0 (in \mathbb{F}_p). So we have a contradiction.

6. PROOF OF THEOREM 2.1 WITH $r \equiv 3 \pmod{p}$

In addition to the common conditions in Theorem 2.1, we assume that $q \geq r^2 - 4r + 5$ and $r \equiv 3 \pmod{p}$. Assume to the contrary that $f = f_{q,r,2,\alpha}$ is a PP of \mathbb{F}_{q^2} .

By (5.7), $A_1(r, \mathbf{z}) = \mathbf{z} - 3$, and hence $z = 3$. In this case, $z = 3$ is a common root of $A_\alpha(r, \mathbf{z})$ for $\alpha = 1, 3, 5$, so (5.7) – (5.9) produce no contradiction. In fact, for $r \equiv 3 \pmod{p}$ and $z = 3$, no contradiction can be derived from (3.9) with $\alpha < p$. A special value of α needs to be considered.

Write $r = kp^l + 3$, where $k, l > 0$, $p \nmid k$. Choose $\alpha = p^l$. Then in (3.3),

$$c = \left\lceil \frac{(r-2)\alpha + r}{q+1} \right\rceil \leq \left\lceil \frac{(r-2)(r-3) + r}{q+1} \right\rceil = \left\lceil \frac{r^2 - 4r + 6}{q+1} \right\rceil \leq 1.$$

So $c = 1$ and

$$(6.1) \quad \frac{d}{2} = \frac{q+1}{2} + \alpha - r \frac{\alpha+1}{2} = \frac{q+1}{2} + p^l - r \frac{p^l+1}{2}.$$

It is clear from (6.1) that $d < q - 1$. Since

$$\binom{\alpha}{i} = \begin{cases} 1 & \text{if } i = 0 \text{ or } p^l, \\ 0 & \text{otherwise,} \end{cases}$$

(3.9) gives

$$0 = \binom{\frac{d}{2}}{p^l} + \binom{\frac{d}{2} + \frac{1}{2}}{p^l} z - \binom{p^l + \frac{d}{2}}{p^l} z^{2p^l} - \binom{p^l + \frac{d}{2} + \frac{1}{2}}{p^l} z^{2p^l+1}.$$

By (6.1), the above equation becomes

(6.2)

$$\binom{u_1 - r \frac{p^l+1}{2}}{p^l} + \binom{u_2 - r \frac{p^l+1}{2}}{p^l} z - \binom{u_3 - r \frac{p^l+1}{2}}{p^l} z^{2p^l} - \binom{u_4 - r \frac{p^l+1}{2}}{p^l} z^{2p^l+1} = 0,$$

where $u_1 = \frac{1}{2} + p^l$, $u_2 = 1 + p^l$, $u_3 = \frac{1}{2} + 2p^l$, $u_4 = 1 + 2p^l$. Since $z = 3$, by (3.11), we know that (6.2) also holds with r replaced by 3, that is,

$$(6.3) \quad \binom{u_1 - 3\frac{p^l+1}{2}}{p^l} + \binom{u_2 - 3\frac{p^l+1}{2}}{p^l}z - \binom{u_3 - 3\frac{p^l+1}{2}}{p^l}z^{2p^l} - \binom{u_4 - 3\frac{p^l+1}{2}}{p^l}z^{2p^l+1} = 0.$$

For $1 \leq i \leq 4$, since

$$u_i - 3\frac{p^l+1}{2} - \left(u_i - r\frac{p^l+1}{2}\right) = kp^l\frac{p^l+1}{2} \equiv \frac{k}{2}p^l \pmod{p^{l+1}},$$

we have

$$\binom{u_i - 3\frac{p^l+1}{2}}{p^l} - \binom{u_i - r\frac{p^l+1}{2}}{p^l} \equiv \frac{k}{2} \pmod{p}.$$

Thus, subtracting (6.2) from (6.3) gives

$$0 = \frac{k}{2}(1 + z - z^{2p^l} - z^{2p^l+1}) = \frac{k}{2}(1 + z)^{p^l+1}(1 - z)^{p^l}.$$

Therefore $z = \pm 1$, which is a contradiction.

7. PROOF OF THEOREM 2.1 WITH $r \not\equiv 3 \pmod{p}$ AND EITHER $p = 3$ OR $r \equiv 7/4 \pmod{p}$

We assume that $q \geq 8r - 15$, $r \not\equiv 3 \pmod{p}$, and either $p = 3$ or $r \equiv 7/4 \pmod{p}$. Again, assume to the contrary that $f = f_{q,r,2,a}$ is a PP of \mathbb{F}_{q^2} .

7.1. The case $p = 3$.

In this case, (5.7) gives $A_1(r, z) = -rz^2 + z + r$. Recall that $\frac{1}{3}A_3(r, z) \in \mathbb{Z}[z]$. Write $r \equiv r_0 \pmod{3^2}$, where $1 \leq r_0 \leq 8$, $3 \nmid r_0$. Then $\frac{1}{3}A_3(r, z) \equiv \frac{1}{3}A_3(r_0, z) \pmod{3}$. Therefore,

$$\text{Res}_{\mathbb{F}_3[z]} \left(A_1(r, z), \frac{1}{3}A_3(r, z) \right) = \text{Res}_{\mathbb{F}_3[z]} \left(A_1(r_0, z), \frac{1}{3}A_3(r_0, z) \right),$$

which is obtained by setting $r = r_0$ in (5.10). It turns out that

$$\text{Res}_{\mathbb{F}_3[z]} \left(A_1(r, z), \frac{1}{3}A_3(r, z) \right) = \begin{cases} 0 & \text{if } r_0 = 4, \\ 1 & \text{if } r_0 = 5, 8, \\ -1 & \text{if } r_0 = 1, 2, 7. \end{cases}$$

It is easy to verify that $A_1(4, z) = -z^2 + z + 1$ divides both $\frac{1}{3}A_3(4, z)$ and $A_5(4, z)$ in $\mathbb{F}_3[z]$. (In fact, $\frac{1}{3}A_3(4, z) = z(z^2 - z - 1)(z^3 - z^2 - z - 1)$ and $\frac{1}{5}A_5(4, z) = z^2(z+1)^2(z^2 - z - 1)$.) This means that the consideration of the sums $\Theta(\alpha)$ in (5.4) – (5.6) with $\alpha = 1, 3, 5$ produces no contradiction.

To extract additional information, we consider (3.9) with $\alpha = 7$. Clearly, $q \geq 8r - 15 \geq 3^2$. In (3.3), we have

$$(7.1) \quad c = \left\lceil \frac{(\alpha+1)r - 2\alpha}{q+1} \right\rceil = \left\lceil \frac{8r - 14}{q+1} \right\rceil$$

and

$$(7.2) \quad \frac{d}{2} = c\frac{q+1}{2} + \alpha - r\frac{\alpha+1}{2} \equiv \frac{c}{2} + 7 - 4 \cdot \frac{7+1}{2} = \frac{c}{2} \pmod{3^2}.$$

Since $q \geq 8r - 15$, (7.1) gives $c = 1$. Note that $d \neq q - 1$. Now (3.9) with $\alpha = 7$ gives

$$(7.3) \quad \Theta(7) := \sum_i \binom{7}{i} (-1)^i \left[\binom{i + \frac{c}{2}}{7} z^{2i} + \binom{i + \frac{c+1}{2}}{7} z^{2i+1} \right] = 0.$$

On the other hand, direct computation shows that

$$(7.4) \quad \Theta(7) := z^6(z+1)A_7(z),$$

where

$$A_7(\mathbf{z}) = (\mathbf{z}^3 - \mathbf{z}^2 - \mathbf{z} - 1)(\mathbf{z}^5 - \mathbf{z}^2 + \mathbf{z} + 1).$$

We must have $A_7(z) = 0 = A_1(4, z) = 0$ in \mathbb{F}_3 . However,

$$\gcd_{\mathbb{F}_3[\mathbf{z}]}(A_1(4, \mathbf{z}), A_7(\mathbf{z})) = 1,$$

which is a contradiction.

Remark 7.1. If $q < 8r - 15$, then for $\alpha = 7$, we have $c = 2$. In this case, (7.4) becomes

$$(7.5) \quad \Theta(7) = z^3(z+1)(z^2 - z - 1)(z^8 + z^5 - z^3 + z^2 + z + 1).$$

Since $A_1(4, z) = -z^2 + z + 1$ appears in (7.5) as a factor, no contradiction is reached.

7.2. The case $r \equiv 7/4 \pmod{p}$.

We may assume that $p > 3$ because of Subsection 7.1. If $p = 5$, then $r \equiv 3 \pmod{p}$, which is false. Therefore, we assume that $p > 5$.

When $r \equiv 7/4 \pmod{p}$, (5.7) – (5.9) in $\mathbb{F}_p[\mathbf{z}]$ becomes

$$(7.6) \quad A_1(r, \mathbf{z}) = \frac{1}{2}(-5\mathbf{z}^2 + 2\mathbf{z} - 1),$$

$$(7.7) \quad A_3(r, \mathbf{z}) = -3\mathbf{z}(5\mathbf{z}^2 - 2\mathbf{z} + 1)(7\mathbf{z}^3 - \mathbf{z}^2 - \mathbf{z} - 1),$$

$$(7.8) \quad A_5(r, \mathbf{z}) = -\frac{5}{2^5}B_5(\mathbf{z}),$$

where

$$(7.9) \quad \begin{aligned} B_5(\mathbf{z}) = & 33649\mathbf{z}^{10} - 19726\mathbf{z}^9 - 2219\mathbf{z}^8 - 1096\mathbf{z}^7 - 1214\mathbf{z}^6 \\ & + 44\mathbf{z}^5 - 814\mathbf{z}^4 + 184\mathbf{z}^3 - 499\mathbf{z}^2 + 114\mathbf{z} - 231. \end{aligned}$$

We find that

$$\text{Res}_{\mathbb{Z}[\mathbf{z}]}(-5\mathbf{z}^2 + 2\mathbf{z} - 1, B_5(\mathbf{z})) = 2^{27} \cdot 3^2 \cdot 181.$$

Thus we must have $p = 181$. In $\mathbb{F}_{181}[\mathbf{z}]$, (7.6) – (7.8) become

$$A_1(r, \mathbf{z}) = 88(\mathbf{z} + 116)(\mathbf{z} + 137),$$

$$A_3(r, \mathbf{z}) = 76\mathbf{z}(\mathbf{z} + 116)(\mathbf{z} + 137)(\mathbf{z} + 159)(\mathbf{z}^2 + 177\mathbf{z} + 67),$$

$$A_5(r, \mathbf{z}) = 178(\mathbf{z} + 116)(\mathbf{z} + 142)$$

$$(\mathbf{z}^8 + 8\mathbf{z}^7 + 163\mathbf{z}^6 + 69\mathbf{z}^5 + 68\mathbf{z}^4 + 165\mathbf{z}^3 + 62\mathbf{z}^2 + 33\mathbf{z} + 152),$$

where the factors in the above are all irreducible in $\mathbb{F}_{181}[\mathbf{z}]$. Since z is a common root of $A_1(r, \mathbf{z})$, $A_3(r, \mathbf{z})$ and $A_5(r, \mathbf{z})$, we must have $\mathbf{z} = -116 = 65$.

As in Subsection 7.1, again we need additional information from (3.9) with $\alpha = 7$. Since $q \geq 8r - 15$, in (3.3), we have $c = 1$ and

$$(7.10) \quad \frac{d}{2} \equiv \frac{c}{2} + 7 - \frac{7}{4} \cdot \frac{8}{2} = \frac{1}{2} \pmod{q}.$$

Note that $d \neq q - 1$ and $q \geq 8r - 15 > 7$. Thus (3.9) (with $\alpha = 7$) and (7.10) imply that

$$\Theta(7) := \sum_i \binom{7}{i} (-1)^i \left[\binom{i + \frac{1}{2}}{7} 65^{2i} + \binom{i + 1}{7} 65^{2i+1} \right] = 0$$

in \mathbb{F}_{181} . However, direct computation gives

$$\Theta(7) = 46 \neq 0,$$

which is a contradiction.

The proof of Theorem 2.1 is now complete.

REFERENCES

- [1] X. Hou, *A class of permutation binomials over finite fields*, J. Number Theory, **133** (2013), 3549 – 3558.
- [2] X. Hou, *A survey of permutation binomials and trinomials over finite fields*, Proceedings of the 11th International Conference on Finite Fields and Their Applications, Magdeburg, Germany, 2013, Contemporary Mathematics **632**, 177 – 191, 2015.
- [3] X. Hou, *Permutation polynomials over finite fields — a survey of recent advances*, Finite Fields Appl., **32** (2015), 82 – 119.
- [4] X. Hou, *Permutation polynomials of \mathbb{F}_{q^2} of the form $aX + X^{r(q-1)+1}$* , in Contemporary Developments in Finite Fields and Applications, A. Canteaut, G. Effinger, S. Huczynska, D. Panario, L. Storme (eds), World Scientific, New Jersey, 2016, 74 – 101.
- [5] X. Hou and S. D. Lappano, *Determination of a type of permutation binomials over finite fields*, J. Number Theory, **147** (2015), 14 – 23.
- [6] S. D. Lappano, *A note regarding permutation binomials over \mathbb{F}_{q^2}* , Finite Fields Appl. **34** (2015), 153 – 160.
- [7] S. D. Lappano, *A family of permutation trinomials over \mathbb{F}_{q^2}* , preprint.
- [8] M. E. Zieve, *Permutation polynomials on \mathbb{F}_q induced from bijective Rédei functions on subgroups of the multiplicative group of \mathbb{F}_q* , arXiv:1310.0776, 2013.

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF SOUTH FLORIDA, TAMPA, FL 33620

E-mail address: xhou@usf.edu